

### **Abstract**

A secure protocol is provided which uses a Diffie-Hellman type shared secret, but modified such that the two parties may authenticate each other using a shared password. In accordance with the invention, a party generates the Diffie-Hellman value  $g^x$  and combines it with a function of at least the password using a group operation, wherein any portion of a result associated with the function that is outside the group is randomized. The resulting value is transmitted to the other party. The group operation is defined for the particular group being used. Every group has a group operation and a corresponding inverse group operation. Upon receipt of the value, the other party performs the inverse group operation on the received value and the function of at least the password, and removes the randomization of any portion of the result associated with the function that is outside the group, to extract  $g^x$  such that the other party may then generate the shared secret  $g^{xy}$  using its knowledge of  $y$ .

1200-526.APP